ORIGINAL

AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with accounts identified as "porfizaid1984@gmail.com," "porfizaid84@gmail.com," and "porfizaid@gmail.com" that is stored at premises controlled by Google, Inc.

Case No. M 15 00150

LODGED
2015 FEB -3 PM 2:
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CAL.
LOS ANGELES

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

2015 APR 29 AM 11:51
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CAL.
LOS ANGELES
FILED

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit is incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

You must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

IT IS FURTHER ORDERED that the Provider named in Attachment A shall comply with the further orders set forth in Attachment B, and shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant.

Date and time issued: 2/3/15 - 3:30 pm

Judge's signature

City and state: Los Angeles, California

Paul L. Abrams, U.S. Magistrate Judge
Printed name and title

AUSA: Jeff Mitchell (x0698)

JM

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	*Date and time warrant executed:*	*Copy of warrant ~~and inventory~~ left with:*
M 15 00150	2-4-15 10:11 AM	

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:
[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

1 CD containing contents of porfizaid@gmail.com; porfizaid1984@gmail.com & porfizaid84@gmail.com

FILED
CLERK, U.S. DISTRICT COURT
APR 29 2015
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 4/29/15

Executing officer's signature

Diane Asato SA

Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the accounts identified as "porfizaid1984@gmail.com" (the "SUBJECT ACCOUNT 1"); "porfizaid84@gmail.com" (the "SUBJECT ACCOUNT 2"); "porfizaid@gmail.com" (the "SUBJECT ACCOUNT 3); and collectively referred to as the "SUBJECT ACCOUNTS" that are stored at premises controlled by www.google.com (i.e., Google, Inc.), a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE

1. The search warrant will be presented to personnel of Google, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the agent who serves the search warrant.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). In conducting this search, the search team shall take notes regarding how it conducts the search.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the

items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 60 days from the date of receipt from the PROVIDER of the response to this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 60-day period.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNTS, limited to that which occurred on or after August 11, 2014 for SUBJECT ACCOUNTS 1 and 2; and on or after July 18, 2014 for SUBJECT ACCOUNT 3, including:

i. All e-mails associated with the SUBJECT ACCOUNTS, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, and deleted e-mails, as well as all header information associated with each e-mail, and any related documents or attachments.

ii. All contraband, including sexually explicit pictures and images of children (i.e., child pornography) as defined in Title 18, United States Code, Section 2256(8).

iii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNTS, including address books, contact and buddy lists, calendar data, pictures, notes, texts, links, user profiles, account settings, access logs, and files.

iv. All instant messaging or "chat" histories, including stored or preserved copies of instant messages or

chats sent to and from the accounts, draft instant messages or chats, and deleted instant messages or chats, as well as all header information associated with each instant message or chat.

v. Any communications in any format, seeking to trade, receive, distribute, and/or produce child pornography.

vi. Any communications in any format, which tend to identify any individual or group that possesses child pornography, distributes child pornography, seeks to receive child pornography, and/or produces child pornography.

vii. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNTS, including contacts with support services and records of actions taken.

b. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNTS described above in Section II.10.a, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations.

c. All subscriber information pertaining to the SUBJECT ACCOUNTS, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP

addresses associated with session dates and times, as well as means and source of payment, including detailed billing records.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), and occurring after August 11, 2014 (for SUBJECT ACCOUNTS 1 and 2), and occurring after July 18, 2014, (for SUBJECT ACCOUNT 3), namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNTS, including records about their identities and whereabouts.

ii. Information relating to the possession, distribution, receipt, production, and/or advertisement of child pornography using the SUBJECT ACCOUNTS.

iii. Information relating to the molestation of children.

iv. Information relating to any potential meeting places and times related to the exchange, possession, or distribution of child pornography, i.e. addresses, cross-streets, intersections, and/or business names.

v. Information relating to children, including discussions that are sexual in nature.

vi. All contraband, including sexually explicit pictures and images of children (i.e., child pornography) as defined in Title 18, United States Code, Section 2256(8).

vii. Any communications in any format, seeking to trade, receive, distribute, and/or produce child pornography.

viii. Any communications in any format, which tend to identify any individual or group which possesses child pornography, distributes child pornography, seeks to receive child pornography, and/or produces child pornography.

b. All records and information described above in Sections II.10.b and II.10.c.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. Notwithstanding 18 U.S.C. § 2252A, the PROVIDER shall send such information via express delivery service to:

Diane Asato
501 West Ocean Boulevard, Suite 7200
Long Beach, California 90802
Phone: (562) 624-4043 Fax: (562) 980-3242
Diane.e.Asato@ice.dhs.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

14. IT IS FURTHER ORDERED that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant.

AFFIDAVIT

I, Diane Asato, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") in Los Angeles, California, and I have been so employed since June 2003. I am currently assigned to the HSI Los Angeles Child Exploitation Investigations Group ("CEIG"), where I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review various examples of child pornography in all forms of media, including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offense. I make this affidavit based upon my personal knowledge and experience, my review of pertinent documentation, and discussions with other investigating law enforcement officers. The facts in this affidavit come from information obtained in the course of an investigation of an individual named Porfirio Benito DIAZ.

2. I make this affidavit in support of an application for a search warrant for information associated with the accounts

identified as "porfizaid1984@gmail.com" (hereinafter the "SUBJECT ACCOUNT 1"), "porfizaid84@gmail.com" (hereinafter the "SUBJECT ACCOUNT 2"), and "porfizaid@gmail.com" (hereinafter the "SUBJECT ACCOUNT 3) (and collectively referred to as the "SUBJECT ACCOUNTS") that is stored at premises controlled by Google, Inc. (the "PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.[1] The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d) to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items

[1] Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

3. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNTS constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF INVESTIGATION

5. On or about October 26, 2014, Google reported to the National Center for Missing and Exploited Children ("NCMEC") that an individual accessing the Google e-mail accounts identified as "porfizaid1984@gmail.com" (SUBJECT ACCOUNT 1) and "porfizaid84@gmail.com" (SUBJECT ACCOUNT 2) had uploaded an image of child pornography to those e-mail accounts.

6. Subsequently, I learned that on or about August 10, 2014, Google reported to NCMEC that an individual accessing the Google e-mail account identified as "porfizaid@gmail.com"

(SUBJECT ACCOUNT 3) had uploaded an image of child pornography to that e-mail account.

7. As set forth in detail below, images of child pornography were uploaded to the SUBJECT ACCOUNTS. Therefore, there is probable cause to believe that the SUBJECT ACCOUNTS contain evidence of child pornography offenses.

III. DEFINITION OF TERMS

8. The following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "computer" is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

c. The term "e-mail" (electronic mail) is defined as the text messages sent from one person to another via a computer. E-mail can also be sent automatically to a large number of addresses via a mailing list.

d. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university,

employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

e. The terms "jpeg," "jpg," "gif," "bmp," and "art" are defined as graphic image files, namely, pictures.

f. The terms "mpeg," "mpg," "mov," "avi," "rm," and "wmv" are defined as video or movie files. To use these video files, one needs a personal computer or other digital devices with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

g. The term Exchanged Image File Format ("EXIF") is defined as data embedded in digital image files. Information may include dates and times photographs were taken, makes and models of the cameras, technical photograph data such as aperture speed, and Global Positioning System ("GPS") coordinates in latitude and longitude of where the photographs were taken.

h. A "hash value" is a numerical identifier for digital data, such as a particular file. It is obtained by using a mathematical function, often called an algorithm. When a hash value is generated for an image file, any other identical image file will have the same hash value. However, if the data is changed, even very slightly (such as the addition or deletion of a single pixel in an image), the hash value will change. Thus, a hash value can be thought of as a "digital fingerprint"

for data - if two images have the same hash value, there is an extremely high likelihood that the images are the same.

i. Although a photo's hash cannot be used to re-create an image or identify people or items within an image, it can be compared with hashes of other photos as a reliable way to match two different copies of the same image. Hash values can be used in a number of ways to assist law enforcement in investigating child exploitation offenses. For example, in conducting forensics on a computer, law enforcement often runs a "hash value comparison" between files on the suspect's computer and a library of hash values of known images and videos suspected to be child pornography.

IV. STATEMENT OF PROBABLE CAUSE

A. IMAGES OF SUSPECTED CHILD PORNOGRAPHY UPLOADED TO THE SUBJECT ACCOUNTS.

9. Electronic Communication Service Providers are required by law to report incidents of online child sexual exploitation to NCMEC.[2] Google, one such Electronic Communication Service Provider, makes these reports based on information they receive and/or through PhotoDNA.[3]

---

[2] Through its Cyber Tipline and its work as a clearinghouse for illegal child sexual abuse images reported by U.S. electronic services providers, NCMEC has unique insight into the identified images of child sexual abuse being distributed on the Web. NCMEC uses PhotoDNA to help enable Google and others to compare hashes of the photos on their services with hashes NCMEC creates of known images of child pornography.

[3] PhotoDNA refers to a technology developed by Microsoft that computes hash values of images in order to identify alike images. PhotoDNA is primarily used in the prevention of child pornography and works by computing a hash that represents an

(footnote cont'd on next page)

10. On or about December 8, 2014, I received two NCMEC CyberTip reports (2999693 and 2999720) containing information originally reported by Google. The NCMEC CyberTip reports indicated that on or about October 26, 2014, an individual using SUBJECT ACCOUNTS 1 and 2 uploaded an image file titled "14.jpg," suspected of containing child pornography, to SUBJECT ACCOUNTS 1 and 2. Google also provided Internet Protocol ("IP") login records that showed that SUBJECT ACCOUNTS 1 and 2 were accessed from August 11, 2014, to approximately October 26, 2014.

11. On or about December 8, 2014, I reviewed the two CyberTips reports 2999693 and 2999720 and the associated image files, both titled "14.jpg," which were provided to NCMEC by Google. Based on my training and experience, the images associated with CyberTips 2999693 and 2999720, titled "14.jpg," appeared to be the same image, and depicted suspected child pornography. The image file is described as follows: The file titled "14.jpg" is an image file that depicts what appears to be a nude prepubescent minor female approximately five to seven years old, exposing her vaginal area. The minor female is being digitally penetrated in the vagina by what appears to be an adult's hand.

---

image. In the same way that the characteristics of every person's DNA are different, the signature of, or "hash value" for, every image is different, enabling the creation of a hash that can identify an image based on its unique characteristics or its "digital DNA." Although a photo's hash cannot be used to re-create an image or identify people or items within an image, it can be compared with hashes of other photos as a reliable way to match two different copies of the same image.

12. While reviewing CybertTip 2999693, I learned that "porfizaid@gmail.com" ("SUBJECT ACCOUNT 3") was reported by Google as a secondary e-mail account to SUBJECT ACCOUNT 1. Furthermore, NCMEC provided another CyberTip report (report number 2720865) based on the username "Porfizaid."

13. On or about January 8, 2015, I obtained a copy of CyberTip report 2720865, which indicated that on or about August 10, 2014, an individual using SUBJECT ACCOUNT 3 uploaded an image file titled "10-3.jpg," suspected of containing child pornography, to SUBJECT ACCOUNT 3. I reviewed the image file titled "10-3.jpg," and based on my training and experience determined that the image depicted child pornography. The image file is described as follows: Image file "10-3.jpg" contains four photos of what appears to be a nude prepubescent female approximately 9-11 years old engaging in various sex acts. One of the photos depicts a nude minor female with her legs apart inserting a blue foreign object into her vagina. The nude minor female is sitting on the stomach of a nude adult female. The CyberTip report also included IP login records that shows that SUBJECT ACCOUNT 3 was accessed from approximately July 18, 2014, to approximately August 10, 2014.

14. On or about December 8, 2014, I sent the PROVIDER a preservation letter requesting that the records and contents of the SUBJECT ACCOUNTS be preserved for 90 days pursuant to Title 18, United States Code, 2703(f).

because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.

19. I know from my training and experience that the complete contents of an e-mail account may be important to establishing the actual user who has dominion and control of that account at a given time. E-mail accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which e-mail accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an e-mail account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the SUBJECT ACCOUNTS, I am

17. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNTS.

18. In my training and experience, e-mail account users will sometimes communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation

computer keyboard to convey an idea, such as the use of a colon and paren :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an e-mail account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

23. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER under seal until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for the PROVIDER to authenticate information taken from the SUBJECT ACCOUNTS as its business record without the original production to examine. Even if the PROVIDER kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the PROVIDER to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the PROVIDER to examine a particular document found by the search team and confirm that it was a business record of the PROVIDER's taken from the SUBJECT ACCOUNTS.

b. I also know from my training and experience that many e-mail accounts are purged as part of the ordinary course

requesting a warrant requiring the PROVIDER to turn over all information associated with the SUBJECT ACCOUNTS with the date restriction included in Attachment B for review by the search team.

20. Relatedly, the government must be allowed to determine whether other individuals had access to the SUBJECT ACCOUNTS. If the government were constrained to review only a small subsection of an e-mail account, that small subsection might give the misleading impression that only a single user had access to the account.

21. Based on my training and experience, I know that people who upload child pornography images to their e-mail accounts typically use it as a means to trade with other individuals with similar interests. Individuals who trade child pornography also use various communication methods such as instant messaging, chat rooms, forums and etc.

22. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of e-mail conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an e-mail or the manipulation and combination of keys on the

by destroying or moving other evidence, or otherwise masking their activity.

VII. CONCLUSION

25. Based on the foregoing, I request that the Court issue the requested search warrant.

Diane Asato, Special Agent
DEPARTMENT OF HOMELAND SECURITY, HOMELAND SECURITY INVESTIGATIONS

Subscribed to and sworn before me on January ___, 2015.

HONORABLE PAUL L. ABRAMS
UNITED STATES MAGISTRATE JUDGE

of business by providers. For example, if an e-mail account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an e-mail account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her e-mail account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

VI. REQUEST FOR NON-DISCLOSURE

24. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscriber(s) of the SUBJECT ACCOUNTS, of the existence of the warrant because there is reason to believe that such notification will result in (1) flight from prosecution; (2) destruction of or tampering with evidence; or (3) otherwise seriously jeopardizing the investigation. The extent of the current investigation set forth above is not public, and I know, based on my training and experience, that individuals who become aware that they are targets of an investigation may flee prosecution. In addition, particularly where evidence of possession of child pornography may be within the SUBJECT ACCOUNTS, if the subscriber(s) learn of this warrant, they may destroy the digital evidence contained within the SUBJECT ACCOUNTS, or otherwise jeopardize the investigation

V. BACKGROUND REGARDING E-MAIL AND THE PROVIDER

15. In my training and experience, I have learned that the PROVIDER provides a variety of online services, including e-mail, to the public. The PROVIDER allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the SUBJECT ACCOUNTS. Subscribers obtain an account by registering with the PROVIDER. During the registration process, the PROVIDER asks subscribers to provide basic personal information. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.

16. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNTS.